RSA® ARCHER®
GRC Platform
Implementation Guide

Securonix Snypr 6.0

Jeffrey Carlson, RSA Partner Engineering
Last Modified: August 2nd, 2017

RSA READY

Solution Summary

Securonix Snypr sends out CEF formatted violation events into the Unified Log Collector of RSA Security Operations Management. These CEF formatted events are forwarded to the RSA Archer GRC Platform as Security Alerts. Security Alerts are aggregated by user into a Security Incident.

Partner Integration Overview	
GRC Use Case	Security Operations and Breach Management
Uses Out Of The Box Applications	Security Incidents, Security Alerts
Uses Custom Application	No
Requires On-Demand License	No

This solution requires access to RSA Archer Security Operations Management 1.3.1. For more information on this offering, consult the RSA Archer Customer/Partner Community at:

https://community.rsa.com/docs/DOC-44272

RSA Archer Configuration

Unified Log Collector (UCF) Configuration

In order for Securonix to send events to UCF, it must be added using the **Generic SEIM Tool** functionality of UCF (see the section entitled **Configure a Generic SEIM Tool** in the *RSA Archer Security Operations Management 1.3 SP1 Installation and Configuration Guide* for more information.) To do this, perform the following steps:

1. Edit the **message-script-identifier.js** file in the <install_dir>\SA IM integration service\config\mapping\scripts folder as follows:

   The securonix log is in the CEF format, so add an **else if** condition in the script under the **scriptIdentifier** function, below the other else ifs added for Splunk, Arcsight and so on. This else if that you add must be present within the **if(splitString.length>3)** loop.
   else if (siemVendor == "HPE"){ scriptResponse = buildReponse("securonix.js","Securonix","2");

```
var scriptIdentifier = function(message){
    var scriptResponse = new Object();
    if(message.indexOf('CEF:')>=0){
        // format Jan 18 11:07:53 host CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|[Extension]
        var beginIndex = message.indexOf('CEF:');
        var cefmessage = message.substring(beginIndex);
        var splitString = cefmessage.split("|")
        // print(splitString.length);
        if(splitString.length>3){
            var siemVendor = splitString[1];
            var siemProduct = splitString[2];
            print(siemProduct);
            if(siemProduct == "Security Analytics (ESA)"){
                scriptResponse = buildReponse("saesa.js","Security Analytics Event Stream Analysis","3");
            }else if(siemProduct == "Splunk"){
                scriptResponse = buildReponse("splunk.js","Splunk","2");
            }else if(siemProduct == "ArcSight"){
                scriptResponse = buildReponse("arcsight.js","Arcsight","2");
            }else if(siemProduct == "Security Analytics (RE)"){
                scriptResponse = buildReponse("sare.js","Security Analytics Reporting Engine","2");
            }else if(siemVendor == "McAfee" && siemProduct == "ESM"){
                scriptResponse = buildReponse("mcafee-esm.js","McAfeeESM","2");
            }
            else if(siemVendor == "HPE"){
                scriptResponse = buildReponse("securonix.js","Securonix","2");
            }
        }

    }else{
```

   If you are using **Securonix** instead of **HP UBA**, then change your **siemVendor** in the above string from **HPE** to **Securonix.**

2. Rename the **securonix.txt** file to **securonix.js**, and place it in the <install_dir>\SA IM integration service\config\mapping\scripts folder.

Note: The **accountName** field of Securonix is mapped to **aggregationcriteria** by default. If the aggregationcriteria (in the CEF) contains the field **Unknown**, then in the securonix.js file aggregationcriteria is mapped to the **src** field in CEF. If src is empty, aggregationcriteria is mapped to the **dst** field in CEF. Lastly, if dst is also empty, then the aggregationcriteria will continue to remain **Unknown** and all alerts with aggregationcriteria containing the field **Unknown** will get aggregated to a **single incident** on Archer GRC.

RSA Archer Application Field Configuration

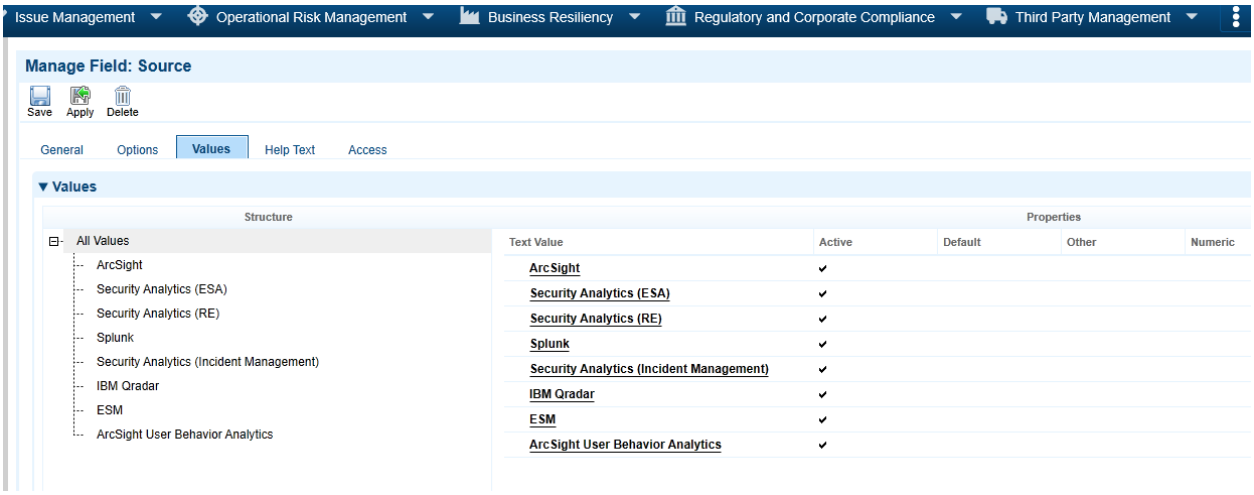
Adding a Value to the Source Field in Security Alerts

In order to list Securonix as a source for incoming alerts, it is first necessary to edit the Source field in the Security Alerts application. To do this, perform the following steps:

1. On the Administration tab, click **Application Builder > Applications**.
2. Open the application **Security Alerts**.
3. On the **Field** tab, click the **Source** field.
4. On the **Values** tab, click **Add New**.
5. Enter the Text Value as:

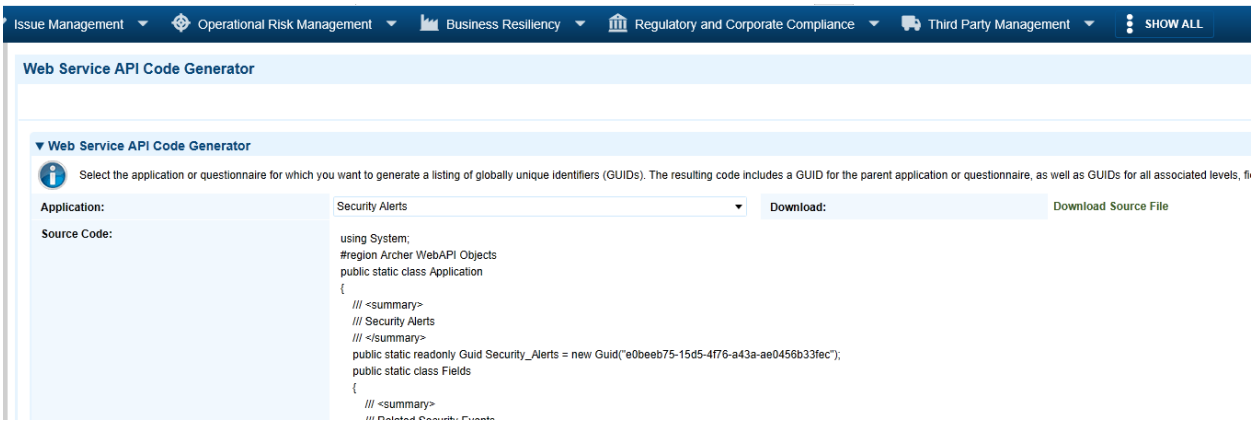
   ArcSight User Behavior Analytics if the vendor is **HPE**.

   Risk and Threat Intelligence if the vendor is **Securonix.**
6. Click **Save**.
7. Click **Save** for the field and the application to commit the new value to the field and application.



8. Extract the GUID of the newly created Source value from RSA Archer GRC as follows:
   a. On the **Administration** tab, click **Integration>Obtain API Resources > Generate API Code**.
   b. Select the application **Security Alerts**.
   c. Click **Download Source File**.
   d. Open the **Security_Alerts.cs** file.
   e. Search for the newly created Source value - **ArcSight User Behavior Analytics**(**Risk and Threat Intelligence** in the case of Securonix).

Note: The value has a corresponding GUID (for reference: %GUID%) associated with it, which is used to configure the mapping file. Example: public static read only Guid ArcSight_User_Behavior_Analytics=new Guid("aba5af52-024246cf-9df9-212e4dd32c14");



9. Add the value of the Source field in the mapping file in the **Unified Log Collector**, as follows:
   a. In the <install_dir>/SA IM integrationservice/config/mappingfolder, open the **secops_import_archer.xml** file.
   b. Navigate to the **Source** field under the **Generic2_SecurityAlerts** application mappings.
   c. In <valueFieldUUIDs> for Source field, add another element for **ArcSight User Behavior Analytics**(**Risk and Threat Intelligence** in the case of Securonix)

      <valueFieldUUID name="ArcSight User Behavior Analytics">%GUID%</valueFieldUUID>

      The GUID must be the GUID obtained from the Step 8 above.

```
<field name="Source">
        <UUID>abc9db3a-60c4-435e-8676-a6f4ee3ab76f</UUID>
        <fieldType>VALUES_LIST</fieldType>
        <keyName>generic.Device Product</keyName>
        <valueFieldUUIDs>
                <valueFieldUUID name="Security Analytics (RE)">0c4d21db-a2ac-4342-8af7-82891430ac5e</valueFieldUUID>
                <valueFieldUUID name="ArcSight">15753f9e-6fad-457b-9dda-e3ab262f82ce</valueFieldUUID>
                <valueFieldUUID name="Splunk">5cfebd1d-005b-4d27-ba78-7537c7f90478</valueFieldUUID>
                <valueFieldUUID name="Security Analytics (ESA)">c6fcf78a-081e-4a70-a40f-6ffc14bd27c6</valueFieldUUID>
                <valueFieldUUID name="IBM QRadar">b115c1b4-ed92-4be8-904c-4b8a08985a76</valueFieldUUID>
                <valueFieldUUID name="ESM">6d732431-e467-4c9e-a2a3-839ccb10e79b</valueFieldUUID>
                <valueFieldUUID name="ArcSight User Behavior Analytics">51835592-82bc-472b-a1a3-bb3afaa4fca7</valueFieldUUID>
        </valueFieldUUIDs>
</field><!--Cross referencing-->
```

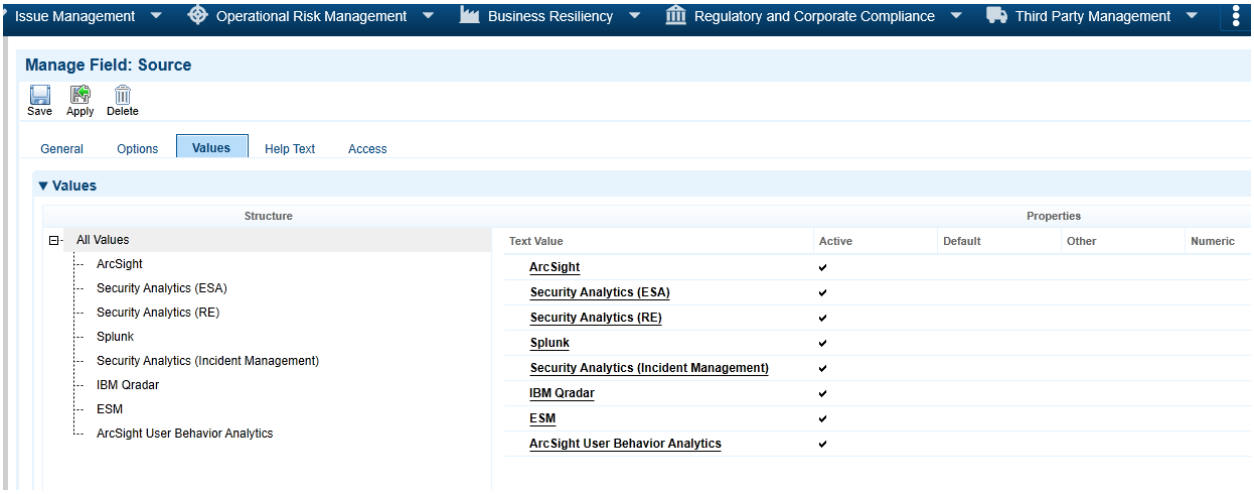
Adding a Value to the Source Field in Security Incidents

In order to list Securonix as a source for incoming incidents, it is first necessary to edit the **Source** field in the **Security Incidents** application. To do this, perform the following steps:

1. On the **Administration** tab, click **Application Builder > Applications**.
2. Open the application **Security Incidents**.
3. On the **Field** tab, click the **Source** field.
4. On the **Values** tab, click **Add New**.
5. Enter the Text Value as:

   ArcSight User Behavior Analytics if the vendor is **HPE**.

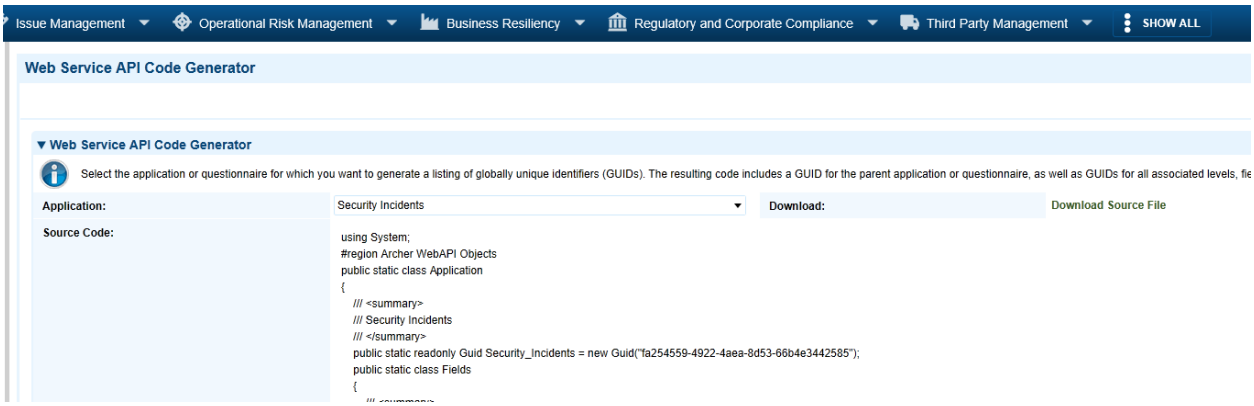
   Risk and Threat Intelligence if the vendor is **Securonix.**
6. Click **Save**.
7. Click **Save** for the field and the application to commit the new value for the field and application.



8. Extract the GUID of the newly created Source value from RSA Archer GRC as follows:
   a. On the **Administration** tab, click **Integration>Obtain API Resources > Generate API Code**.
   b. Select the application **Security Incidents**.
   c. Click **Download Source File**.
   d. Open the **Security_Incidents.cs** file.
   e. Search for the newly created Source value - - **ArcSight User Behavior Analytics**(**Risk and Threat Intelligence** in the case of Securonix).

      Note: The value has a corresponding GUID (for reference: %GUID%) associated with it, which is used to configure the mapping file. Example: public static read only Guid

ArcSight_User_Behavior_Analytics=new Guid("aba5af52-024246cf-9df9-212e4dd32c14");



9. Add the value of the **Source** field in the mapping file in the **Unified Log Collector**, as follows:
    a. In the <install_dir>/SA IM integrationservice/config/mappingfolder, open the **secops_import_archer.xml** file.
    b. Navigate to the **Source** field under the **Generic2_SecurityIncidents** application mappings.
    c. In <valueFieldUUIDs> for Source field, add another element for **ArcSight User Behavior Analytics**(**Risk and Threat Intelligence** in the case of Securonix)

    <valueFieldUUID name="ArcSight User Behavior Analytics">%GUID%</valueFieldUUID>

    The GUID must be the GUID obtained from the Step 8 above.

```
<field name="Source">
        <UUID>abc9db3a-60c4-435e-8676-a6f4ee3ab76f</UUID>
        <fieldType>VALUES_LIST</fieldType>
        <keyName>generic.Device Product</keyName>
        <valueFieldUUIDs>
                <valueFieldUUID name="Security Analytics (RE)">0c4d21db-a2ac-4342-8af7-82891430ac5e</valueFieldUUID>
                <valueFieldUUID name="ArcSight">15753f9e-6fad-457b-9dda-e3ab262f82ce</valueFieldUUID>
                <valueFieldUUID name="Splunk">5cfebd1d-005b-4d27-ba78-7537c7f90478</valueFieldUUID>
                <valueFieldUUID name="Security Analytics (ESA)">c6fcf78a-081e-4a70-a40f-6ffc14bd27c6</valueFieldUUID>
                <valueFieldUUID name="IBM QRadar">b115c1b4-ed92-4be8-904c-4b8a08985a76</valueFieldUUID>
                <valueFieldUUID name="ESM">6d732431-e467-4c9e-a2a3-839ccb10e79b</valueFieldUUID>
                <valueFieldUUID name="ArcSight User Behavior Analytics">51835592-82bc-472b-a1a3-bb3afaa4fca7</valueFieldUUID>
        </valueFieldUUIDs>
</field><!--Cross referencing-->
```

Adding Additional Securonix Fields to RSA Archer

In order to receive the full details for Securonix alert, it is also necessary to create a number of custom fields in the **Security Alerts** application. The steps for this are as follows:

Source UID

1. On the **Administration** tab, click **Application Builder > Applications**.
2. Open the application **Security Alerts**.
3. On the **Field** tab, click **Add New**.
4. Select the radio button **Create a new field from scratch** and set the field type as **Text**.
5. Type **Source UID** for the name of the field.
6. Click **Save**.
7. On the Administration tab, click Application Builder > Applications.
8. Open the application Security Incidents.
9. On the Field tab, click the **Source UID**.
10. Copy the **ID** field.
11. In the UCF, In the <install_dir>/SA IM integrationservice/config/mappingfolder, open the **secops_import_archer.xml** file.
    a. Create a new field under the **Generic2_SecurityAlerts** application mappings as follows:

    <field name="Source UID">

    <UUID>2507D1BE-7BCB-4DF1-B0E6-0CEC7C466C3A</UUID>

    <fieldType>TEXT</fieldType>

    <keyName>generic.suid</keyName>

    </field>

    b. Replace the UUID with the ID copied from step j. above.

Destination UID

1. Follow steps 1-10 above, substituting **Destination UID** as the field name.
2. In the UCF, in the <install_dir>/SA IM integrationservice/config/mappingfolder, open the **secops_import_archer.xml** file.
    a. Create a new field under the **Generic2_SecurityAlerts** application mappings as follows:

    <field name=" Destination UID">

    <UUID>2507D1BE-7BCB-4DF1-B0E6-0CEC7C466C3A</UUID>

    <fieldType>TEXT</fieldType>

<keyName>generic.duid</keyName>

</field>

b. Replace the UUID with the ID copied from the field definition in Archer.

User First Name

1. Follow steps 1-10 from **Source UID** above, substituting **User First Name** as the field name.
2. In the UCF, in the <install_dir>/SA IM integrationservice/config/mappingfolder, open the **secops_import_archer.xml** file.
    a. Create a new field under the **Generic2_SecurityAlerts** application mappings as follows:

    <field name="User First Name">

    <UUID>2507D1BE-7BCB-4DF1-B0E6-0CEC7C466C3A</UUID>

    <fieldType>TEXT</fieldType>

    <keyName>generic.First Name</keyName>

    </field>

    b. Replace the UUID with the ID copied from the field definition in Archer.

User Last Name

1. Follow steps 1-10 from **Source UID** above, substituting **User Last Name** as the field name.
2. In the UCF, in the <install_dir>/SA IM integrationservice/config/mappingfolder, open the **secops_import_archer.xml** file.
    a. Create a new field under the **Generic2_SecurityAlerts** application mappings as follows:

    <field name="User Last Name">

    <UUID>2507D1BE-7BCB-4DF1-B0E6-0CEC7C466C3A</UUID>

    <fieldType>TEXT</fieldType>

    <keyName> generic.Last Name</keyName>

    </field>

    b. Replace the UUID with the ID copied from the field definition in Archer.

User Job Title

1. Follow steps 1-10 from **Source UID** above, substituting **User Job Title** as the field name.
2. In the UCF, in the <install_dir>/SA IM integrationservice/config/mappingfolder, open the **secops_import_archer.xml** file.
    a. Create a new field under the **Generic2_SecurityAlerts** application mappings as follows:

<field name="User Job Title">

<UUID>2507D1BE-7BCB-4DF1-B0E6-0CEC7C466C3A</UUID>

<fieldType>TEXT</fieldType>

<keyName> generic.Job Title</keyName>

</field>

b. Replace the UUID with the ID copied from the field definition in Archer.

User Employee ID

1. Follow steps 1-10 from **Source UID** above, substituting **User Employee ID** as the field name.
2. In the UCF, in the <install_dir>/SA IM integrationservice/config/mappingfolder, open the **secops_import_archer.xml** file.
    a. Create a new field under the **Generic2_SecurityAlerts** application mappings as follows:

    <field name="User Employee ID">

    <UUID>2507D1BE-7BCB-4DF1-B0E6-0CEC7C466C3A</UUID>

    <fieldType>TEXT</fieldType>

    <keyName>generic.Employee ID</keyName>

    </field>

    b. Replace the UUID with the ID copied from the field definition in Archer.

User Department

1. Follow steps 1-10 from **Source UID** above, substituting **User Department** as the field name.
2. In the UCF, in the <install_dir>/SA IM integrationservice/config/mappingfolder, open the **secops_import_archer.xml** file.
    a. Create a new field under the **Generic2_SecurityAlerts** application mappings as follows:

    <field name="User Department">

    <UUID>2507D1BE-7BCB-4DF1-B0E6-0CEC7C466C3A</UUID>

    <fieldType>TEXT</fieldType>

    <keyName> generic.Department</keyName>

    </field>

    b. Replace the UUID with the ID copied from the field definition in Archer.

Manager Employee ID

1. Follow steps 1-10 from **Source UID** above, substituting **Manager Employee ID** as the field name.
2. In the UCF, in the <install_dir>/SA IM integrationservice/config/mappingfolder, open the **secops_import_archer.xml** file.
    a. Create a new field under the **Generic2_SecurityAlerts** application mappings as follows:

    <field name="Manager Employee ID">

    <UUID>2507D1BE-7BCB-4DF1-B0E6-0CEC7C466C3A</UUID>

    <fieldType>TEXT</fieldType>

    <keyName>generic.Manager Employee ID</keyName>

    </field>

    b. Replace the UUID with the ID copied from the field definition in Archer.

Violation Risk Score

1. Follow steps 1-10 from **Source UID** above, substituting **Violation Risk Score** as the field name.
2. In the UCF, in the <install_dir>/SA IM integrationservice/config/mappingfolder, open the **secops_import_archer.xml** file.
    a. Create a new field under the **Generic2_SecurityAlerts** application mappings as follows:

    <field name=”Violation Risk Score">

    <UUID>2507D1BE-7BCB-4DF1-B0E6-0CEC7C466C3A</UUID>

    <fieldType>TEXT</fieldType>

    <keyName>generic.Violation Risk Score</keyName>

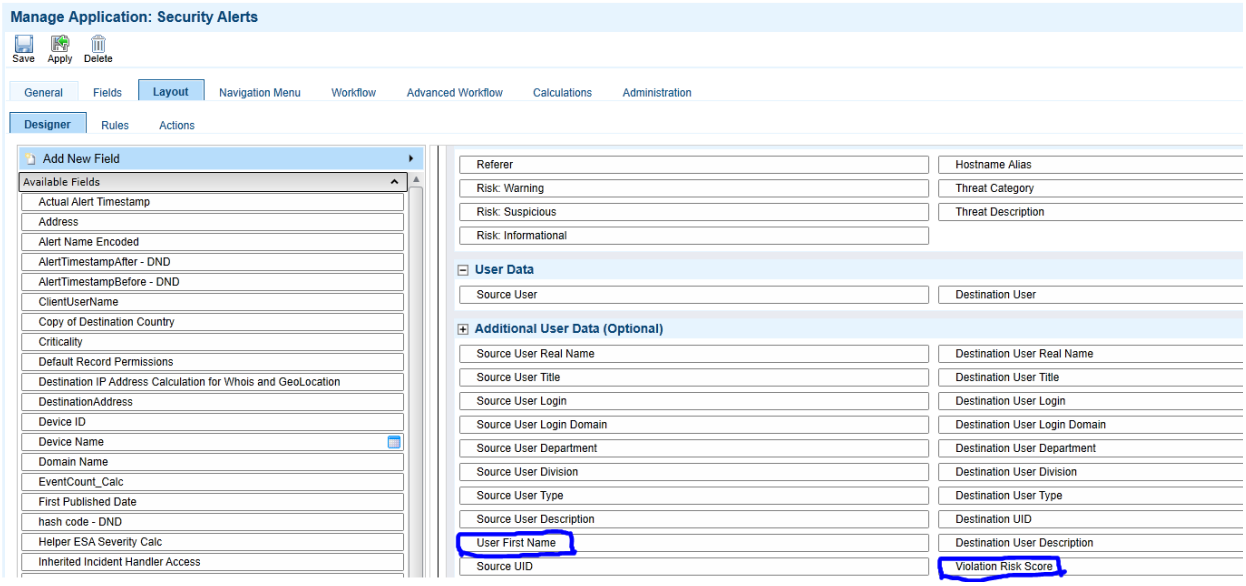
    </field>

    b. Replace the UUID with the ID copied from the field definition in Archer.

Adding New Felds to the Layout

Now that these custom fields have been created, it will be necessary to add them to the layout in order to see their values. To do this, perform the following steps:

1. On the **Administration** tab, click **Application Builder > Applications**.
2. Open the application **Security Alerts**.
3. Go to the **Layout** tab and drag and drop all the newly created fields from the left onto the position that you want them on the screen.



4. Save the application to ensure the desired changes are persisted. Also, be sure to restart the Unified Log Collector before ingesting any alerts.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring Securonix Snypr with RSA Archer. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

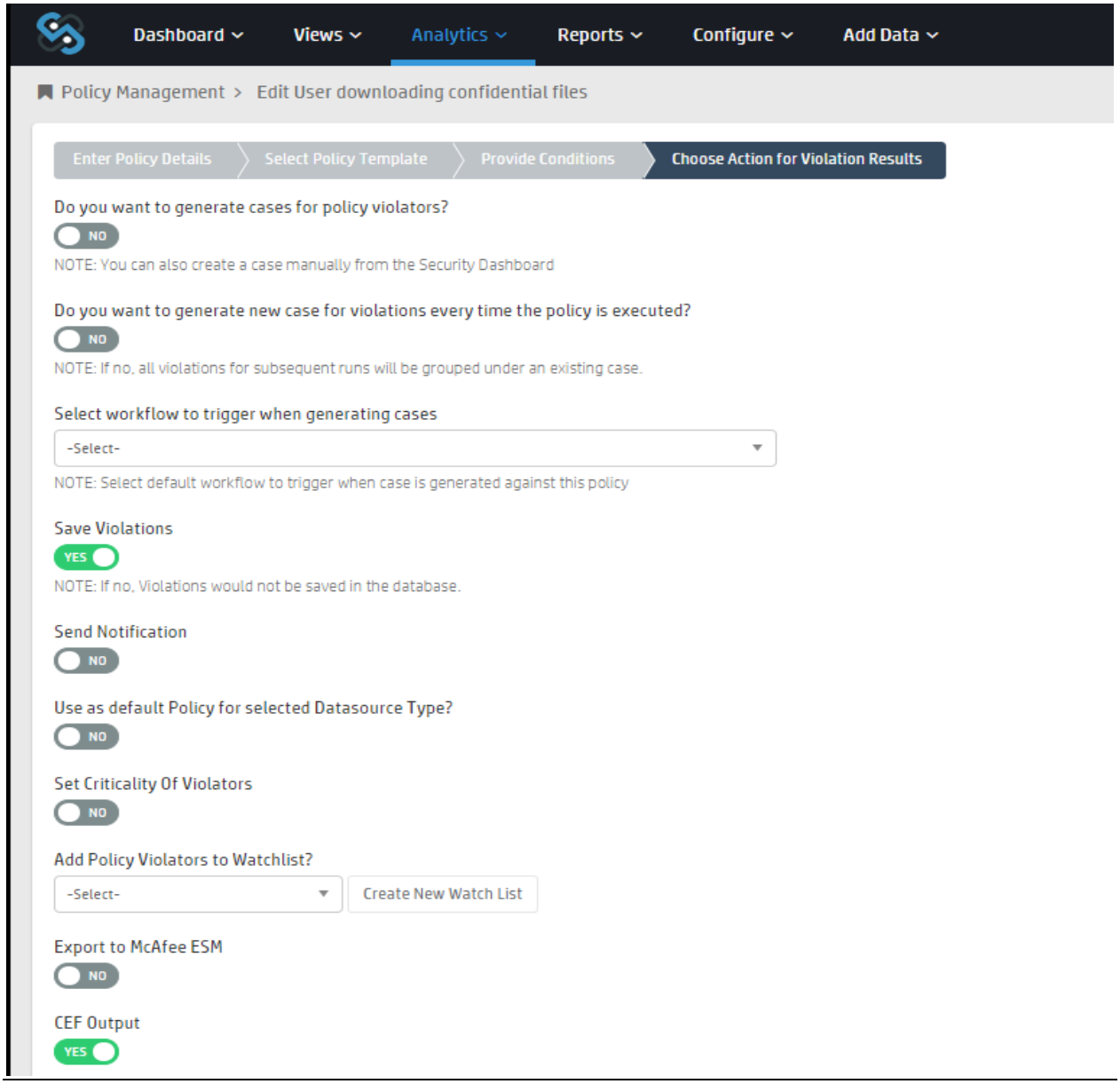
All Snypr components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

> **Important: The configuration shown in this Implementation Guide is for example and testing purposes only. It is not intended to be the optimal setup for the device. It is recommended that customers make sure Securonix Snypr is properly configured and secured before deploying to a production environment. For more information, please refer to the Securonix Snypr documentation or website.**

Securonix Snypr Configuration

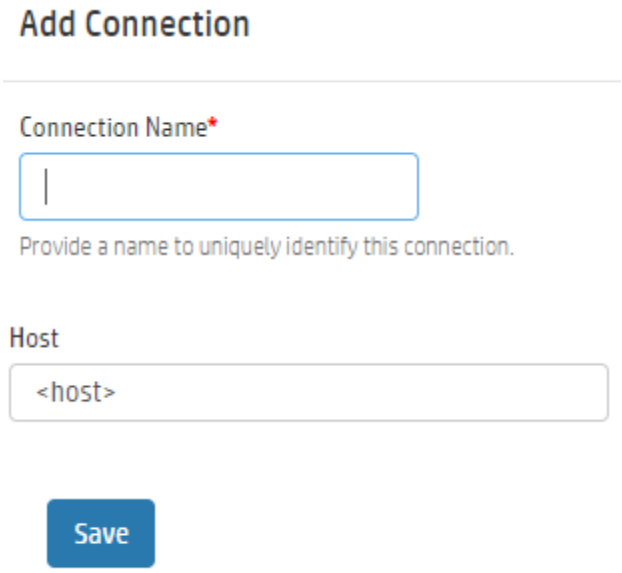
Select the policy in Snypr for which you want to edit and send CEF formatted alerts to RSA Archer GRC.

1. In the 4th step – Choose Action For Violation Results, enable the **CEF Ouput** button.



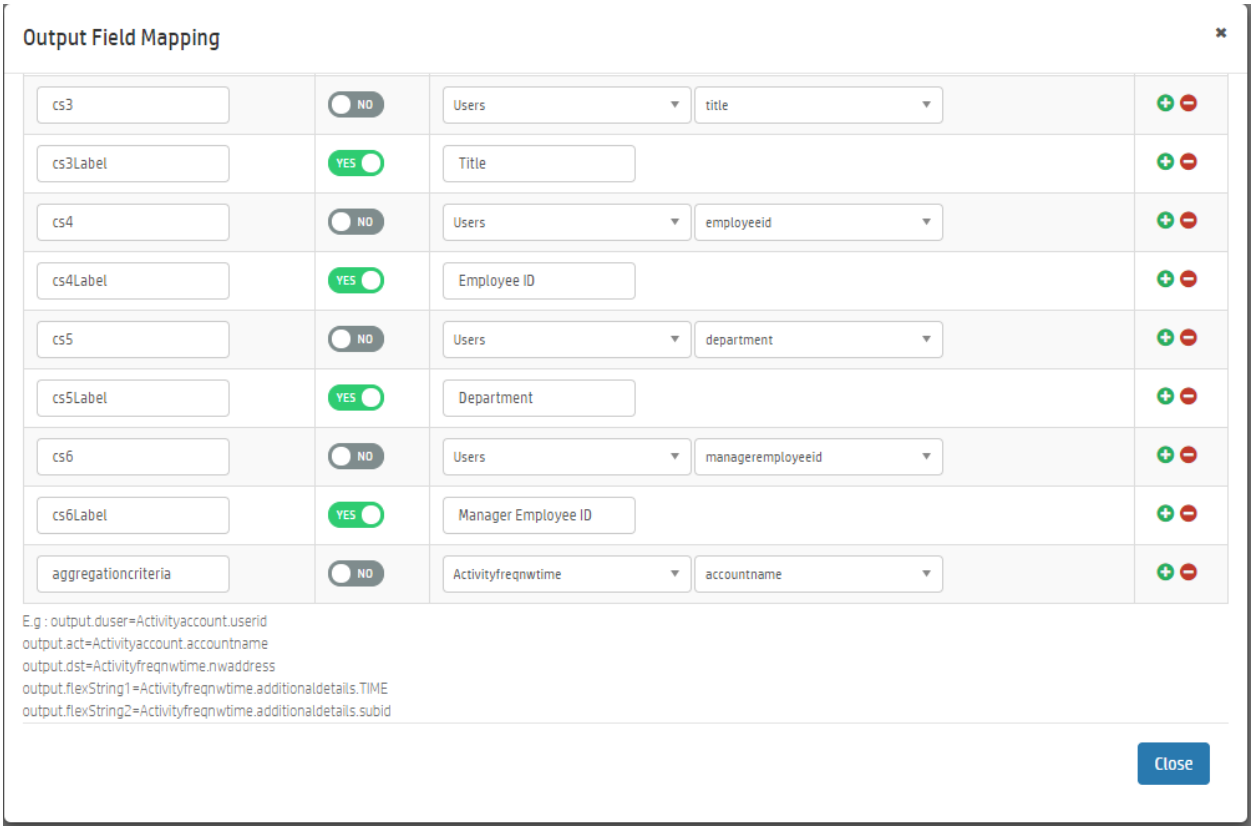
This opens up a new box below,

2. In the drop down, select **Create New Connection** option. This will open a new screen called **Add Connection**



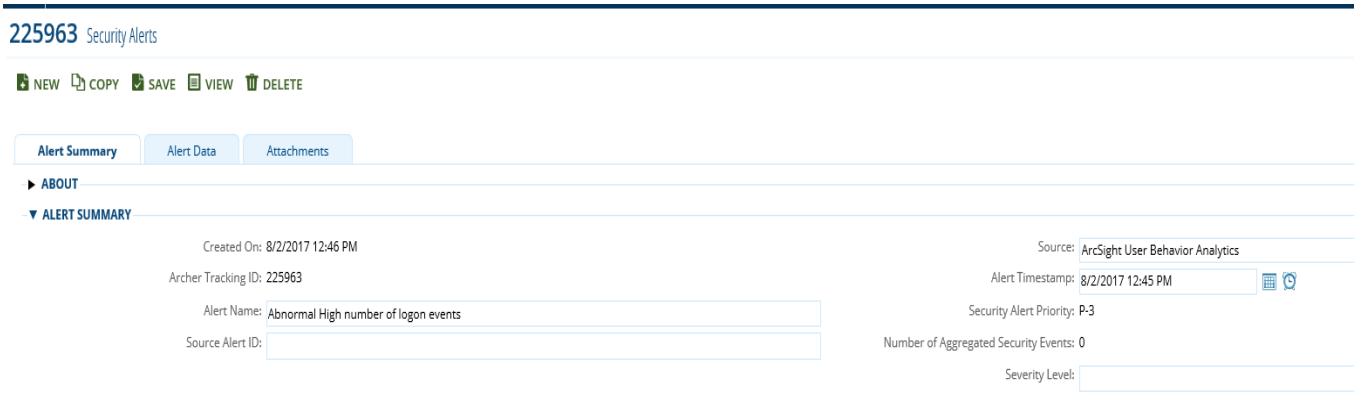
3. Enter a new **Connection Name**, Enter the IP Address of the Unified Log Collector under **Host**, and hit **Save**.

4. Click on the **Output Field Mapping** button, it opens up a new box, there, add a new field called **aggregationcriteria** and map it to the **accountname** field under the **Activityfreqnwtime** table.



5. Now when the policy for which CEF violations are to be sent to Archer GRC is run, the violations are sent directly to Archer GRC as CEF data.

   Below is a sample alert on the RSA Archer GRC system.



Certification Environment for RSA Archer GRC

Date Tested: August 1st, 2017

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Archer GRC	6.2	Windows 2012
RSA Security Operations Management	1.3.1.1	Windows 2012
Securonix Snyper	6.0	